Department of Defense

Concept of Operations

(CONOPS)

for

Director, Information Assurance Division

Office of the Chief Information Officer/G6

Headquarters, Department of the Army

Executive Summary

The goal of the Initiative for State Infrastructure Protection (ISIP) is to assure military mobilization readiness through enhancing civil cyber security. Military mobilization readiness is dependent on ensuring nationwide cyber infrastructure capabilities as well as effective cyber military installation critical infrastructure protection (CIP). Military installation critical infrastructure is dependent on and significantly integrated with civilian cyber resources.

There are two facets to ISIP. First, DoD shares selected cyber resources so as to enhance civil cyber protection capabilities. Second, DoD gleans cyber exploitation information from the civilian agencies and private companies that monitor critical infrastructures. The net effect is that both the states and DoD working together enhance overall infrastructure cyber security.

ISIP establishes a methodology to provide the Department of Defense (DoD) Information Assurance (IA) messages, advisories and alerts from the DoD Computer Emergency Response Team (CERT) to each State National Guard CERT. Each State National Guard CERT may share appropriate cyber information with state government agencies through established linkages. By providing this information to the states, DoD anticipates generating a return information flow of cyber security information from civil cyber security sensors back to DoD. This two-way flow of information can provide early alert and warnings of potential problems and strengthens and protects DoD critical infrastructure systems and facilities.

Pursuant to General Correspondence from the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD-C3I) dated 7 April 2002, the Army CIO/G6 Information Assurance Office assumed oversight responsibility for the Initiative for State Infrastructure Protection. This

Concept of Operations implements the plan for operational oversight of the ISIP program.

Department of Defense
CONCEPT OF OPERATIONS for Initiative For State Infrastructure Protection

1. Introduction

Cyber security information sharing between Federal, State, and Local governments and between government and civilian entities has long been recognized as mutually beneficial (see Presidential Decision Directive 63 and Executive Order 13231). Unfortunately, most information sharing efforts between the Department of Defense (DoD) and other entities are substantially stymied by inertia caused by cultural suspicions, stovepipe organizational relationships, lack of processes, by governmental restrictions on sharing sensitive information and civil concerns over protecting proprietary information.

The exigencies of the Global War on Terrorism resulted in renewed efforts to overcome obstacles and to implement cyber security information sharing. Executive Order 13231 dated October 16, 2001 provides that the Federal government shall "work with industry, state and local governments, and nongovernmental organizations to ensure that systems are created and well managed to share warning, analysis, and recovery information among government network operation centers, information sharing and analysis centers established on a voluntary basis by industry, and other related operations centers." The objectives are to prevent cyber attacks, to reduce national vulnerabilities to cyber attacks, and to minimize the damage and recovery times from such attacks.

This DoD program with the Department of the Army as Action Agent, the Initiative for State Infrastructure Protection, is an innovative program sharing cyber information using the National Guard as the conduit between Federal and State entities. The "dual-hatted" status of the National Guard, federal soldier and state militia, uniquely positions the National Guard to overcome inertia, suspicions, resistance, and handle appropriately classified information restrictions and proprietary concerns

1.1 Background

The concept now known as ISIP was developed by the Defense-wide Information Assurance Program (DIAP) and vetted through an interagency working group that included members from DoD, Department of Commerce, Department of Justice, and the National Infrastructure Protection Center. The breakthrough insight of the initiative is that DoD will provide to state National Guards elements Department of Defense Information Assurance (IA) messages, advisories, and alerts. State National Guard elements may share appropriate cyber information with state agencies through established linkages. ASD-C3I found the working group had produced a mature concept that "requires only final coordination of the information flow processes from the DoD CERT to state National Guard organizations."

A Service was required to take on the responsibility for execution oversight of the final coordination of the information processes. The Army's preeminent Homeland Security role and historical involvement with ISIP made it the logical candidate to assume lead Service oversight responsibility for the required processes to implement ISIP. Pursuant to General Correspondence from ASD-C3I, dated 7 April 2002, the Army was directed to assume oversight responsibility for the Initiative for State Infrastructure Protection (ISIP) (Appendix 1). Accordingly, the Army CIO/G6 IA Office assumed Service oversight responsibility

for the ISIP program. The requirements for ISIP operational oversight are enumerated in a memorandum CIO/G6 dated April 24, 2002 (Appendix 2).

1.2 Responsibilities

Army CIO/G6 IA Division is charged with establishing an interactive process among DoD, state and local levels that share infrastructure cyber protection processes, best practices relevant to national, state, and local levels, critical infrastructure protection (CIP), threat and warning information, and best practices relevant to national, state, and local levels. This process is the Initiative for State Infrastructure Protection (ISIP).

2. Concept

The Defense-wide Information Assurance Program developed the overall concept for ISIP (Appendix 1). The concept was vetted and approved. Army CIO/G6 Information Assurance Office is directed to provide state outreach and implementation of ISIP.

3. State Outreach

The concept for state outreach is to utilize the respective National Guard CERT as the point of contact for dissemination of Department of Defense Information Assurance messages, advisories and alerts from DoD CERT. The National Guard Bureau (NGB) by statute is the exclusive point of contact for all DoD contact with state National Guards. ISIP coordinates with NGB for contact with each of the various state National Guards (54 including Guam, Puerto Rico, Virgin Islands and the District of Columbia). Additional contacts are made directly with non-military state chief information officers (CIO) and through NASCIO (National Association of State Chief Information Officers). ISIP develops contact lists and establishes person-to- person credibility with state points of contact.

3.1. National Guard CERT

The recommended interface with the ISIP program is the National Guard. The National Guard consists of the National Guard Bureau, part of DoD, and the various state and territorial Army/Air National Guard units serving pursuant to Title 32 United States Code. Robust National Guard (NG) Information Assurance (IA) programs are in place at NGB and in the fifty-four National Guards. IA is information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentially, and non-reproduction. The Army National Guard Computer Emergency Response Team/Coordination Center (ARNG-CERT/CC) conducts defensive IA in support of Guard Net XXI and National Guard State Area Command (STARC) level networks. The National Guard is an essential state asset during crisis. The Adjutant General in many states is responsible for emergency response and in all states the National Guard is a vital asset during crisis response. Each National Guard CERT is a key state response asset for cyber related crisis response. National Guard information operations are authorized six hundred and ninety soldiers. Three hundred and seventy-eight are assigned to State National Guard CERTs. Many of these soldiers possess extensive civilian IA experience. To ensure all personnel are trained the ARNG has three Centers of Excellence information operations training centers (Vermont, Virginia, and Washington) and the National Guard Professional Education Center (PEC), Camp Robinson, N. Little Rock, AR.

A state level Computer Emergency Response Team (CERT) is at each of the fifty-four STARC headquarters. Each state level CERT has seven soldiers assigned (four officers and three NCOs) and one full time IA GS-11 position.

4. Stages for the Implementation of ISIP

Implementation of ISIP is envisioned as a multi-year effort and executed through stages. The fifty-four states and territories are each distinct jurisdictions with unique issues and differing capabilities. The stages for implementing ISIP will therefore not be nationwide sequential. Implementation of ISIP must be flexible and adapted to each jurisdiction. Stages for implementation of ISIP are: awareness, buy-in, engagement in mutual information sharing, and education and training.

4.1 Awareness

Creating awareness begins with the initiation of state outreach. Awareness is generated through person-to-person contacts and through media. ISIP team members follow up person-to-person contacts with briefings conducted as part of state outreach efforts. ISIP team members participate and offer briefings at meetings of national organizations serving the state cyber community such as NASCIO, NGA, and other national associations. The IA Division created and maintains an ISIP Web Page (http://www.army.mil/ciog6/isip). The ISIP Web Page provides state contact information, links, news, documents and information about ISIP.

4.2 Buy-In

“Buy-in” is achieved when responsible officers of a state agree to support the implementation of ISIP in their jurisdiction. Buy-in is evidenced by the adoption of mutual goals by the state through the National Guard with ISIP. Participation in the education and training stages of the implementation of ISIP further evidences buy-in.

4.3 Engagement in Mutual Information Sharing

The key indicators of effective engagement in mutual information sharing will be State National Guard CERTs reporting implementation of information assurance vulnerability alerts (IAVAs) technical fixes to DoD CERT and DoD CERT acknowledging state/local furnished through a State National Guard CERT information of a previously unknown threat or vulnerability.

4.4 Education and Training

Education materials, training opportunities and best practices are included on the ISIP homepage. These include cyber security plans developed by states. ISIP relates to other governmental agencies dealing with complimentary critical infrastructure protection challenges. DoD shares with the jurisdictions via the State National Guard CERTs technical information: Information Assurance Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVB), Technical Advisories, and IA training materials/best practices. ISIP team members participate as speakers and visiting instructors as appropriate in education and training of State National Guard CERT members at National Guard Education/Training sites. ISIP will also facilitate identifying appropriate exercise activities for selected states.

4.5 Program Execution

In order to ensure that ISIP is effective in meeting state needs, selected states will be identified to serve as models. Deliberate engagement will be undertaken with a small set of states to determine applicable ISIP procedures and processes.

5. Conclusion

There are many challenges in handling information exchange among federal, state and localities. Many operational, programmatic, and funding activities addressing terrorist attacks are classified because of national security. There are legitimate concerns restricting public disclosure of information regarding vulnerabilities and planned responses. Freedom of information laws and disclosure policies are not uniform amongst the various states and with the federal agencies. Most private sector businesses are hesitant to expose their proprietary secrets and vulnerabilities. Other programs have not overcome the challenge of how to provide for the expedient exchange of appropriate information given a seemingly intractable environment. The relationship between the DoD through the Army in Federal Title 10 status and the National Guard while in a Federal Title 32 status provides a unique ideal conduit for the exchange of such appropriate information.

ISIP provides for transmission of time-sensitive cyber information between federal authorities and National Guard CERTs likewise in federal status with the same security access, but under the command and control of the governor of their respective state. As appropriate, National Guard CERT personnel may serve as two-way conduits for cyber information exchange among the federal, state, and localities. The National Guard CERT members may as appropriate and while not transmitting proprietary secrets, business sensitive vulnerabilities also serve as a two-way conduit for their own civilian acquired cyber information to the federal, state and locality governmental levels. The National Guard soldiers in IA serve as a repository for gleaned cyber information and a filter for the passage of information among local, state, and federal sources for effective cyber Homeland Defense.

ISIP is an essential program to assure cyber readiness for mobilization of the United States military (Regular and Reserve) forces. It will serve as a proactive

measure to mitigate and prevent potential cyber security problems and thus ensure DoD mobilization will occur with minimal disruption. While ISIP shares many facets with civilian Homeland Security cyber readiness efforts it is distinct in its focus on DoD mobilization and will serve as a force multiplier because it enhances civilian cyber infrastructure protection.